GovWorks
FEDERAL ACQUISITION CENTER
Government working with government.

October 27, 2005

INFORMATION REQUEST OR TRANSMITTAL NO. 05-10

TO: Division Chief, Acquisition Management I Division
Division Chief, Acquisition Management II Division
Division Chief, Acquisition Management III Division
Division Chief, Administrative Services Division
Division Chief, Customer Relations Division
Division Chief, Acquisition and Property Management Division

FROM: David Sutfin
Assistant Director, NBC/GovWorks Directorate

SUBJECT: Department of Interior Acquisition Policy Release

PURPOSE: This transmittal provides the Department of Interior's Policy Release, DIAPR 2006-3, on the implementation of Homeland Security Presidential Directive-12 (HSPD-12).

EFFECTIVE DATE: Upon issuance and will remain in effect until canceled, amended or otherwise superseded.

SCOPE: This transmittal applies to all NBC/GovWorks personnel.

BACKGROUND/DISCUSSION:

The Department of Interior (DOI) issued the Department of Interior Acquisition Release (DIAPR) 2006-03 on October 24, 2005. This policy establishes procedures for standard implementation of Homeland Security Presidential Directive (HSPD)-12 for DOI contracts. The HSPD-12 was issued on August 27, 2004, to create a new Federal standard for secure and reliable identification issued by Federal agencies to their employees and contractors. Implementation will occur in several phases. The first phase, put in place on October 27, 2005, was the implementation of procedures for Personal Identity Verification (PIV) credentials such as security badges, building passes, and other procedures. The implementation of later phases will expand coverage to personnel who have been issued credentials as of October 27, 2005, and the use of Smart Cards.

The point of contact for this IRT is Chief, Policy Branch (703) 787-1537.

Attachment 1 – DIAPR 2006-03
Attachment 2 – Financial Assistance
Attachment 3 – Flow Chart
Attachment 4 – Credential Request Form
Attachment 5 – Request for PIV Credential

Attachment 1 – DIAPR 2006-03

October 24, 2005

Department of the Interior Acquisition Policy Release (DIAPR) 2006-03

SUBJECT: Implementation of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors

1. **Purpose**: This policy release establishes procedures for standard implementation of HSPD-12 in DOI contracts.

2. **Effective Date**: Upon signature.

3. **Expiration Date**: Upon revision of the FAR or DIAR.

4. **Background and Explanation**:
HSPD-12, issued on August 27, 2004, directs the creation of a new Federal standard for secure and reliable identification issued by Federal agencies to their employees and contractors, including all tiers of subcontractors. Implementation will be in several stages, with the initial phase being put in place on October 27, 2005. This first phase consists of implementation of procedures under which Personal Identity Verification (PIV) credentials such as security badges, building passes, and so forth, will only be issued after the individual's identity has been independently verified. Later phases will expand coverage to personnel who have already been issued credentials as of October 27, and use of Smart Cards.

Not every contractor and subcontractor (hereafter, "contractor") employee will need PIV credentials. There are two categories of contractor personnel who will be subject to the background investigations:

- Those who need routine and regular unsupervised access to a Federally controlled facility for more than 180 days;
- Those who need any unsupervised access to a Federally controlled Level 3 or 4 information system.

Physical Access. A "Federally controlled facility" is federally owned or leased space, whether for single or multi-tenant occupancy, all or any portion of which is under the jurisdiction, custody or control of DOI. If a building is shared with non-government tenants, only access to the Federal area is controlled. The requirements for contractor credentialing apply even if there is no guard, card reader, or other physical control at the entrance to the office. The 180 calendar day period begins on the first day of the individual's affiliation with DOI (in this case, the date that contract performance begins rather than contract award) and ends exactly 180 days later,

regardless of the number of times the contractor actually accessed a building or IT system.

Logical Access. An "information technology system" is defined in the Federal Information Security Management Act of 2002 (44 U.S.C. §3503(8)). Use of an information system by a contractor on behalf of an agency is defined in 44 U.S.C. §3544(a)(1)(A). If a contractor needs *any* amount of unsupervised access to a DOI IT system, HSPD-12 compliant credentials must be issued regardless of the duration of access. The credentialing requirement applies whether the contractor accesses the IT system from the premises of a DOI facility, from their own facility, through the Internet, or by any other means.

Uncredentialed Contractors. Contractors who do not fit into one of the above two categories will be treated as visitors. This group includes temporary and seasonal workers, and those needing intermittent physical access such as delivery services. These persons must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times. Normally, persons working exclusively outside on the grounds of federally controlled facilities, such as grounds maintenance workers, parking attendants, and some construction workers, need not receive background investigations.

Special Cases. The preceding paragraphs describe the minimum requirements. Depending on risk, increased application of HSPD-12 will be appropriate in some cases. Workers at construction sites may or may not need PIV credentials depending on the nature of what is being built. For example, it may be appropriate to credential workers on a critically sensitive dam. Similarly, even grounds workers at a sensitive site, such as the White House, should be credentialed. If higher level security, such as Secret or Top Secret, is needed, other clearances can be added to the HSPD-12 requirements.

Verification Process. To the extent possible, HSPD-12 clearance of contractor personnel will be handled through the same procedures as for employees. The process has two steps: a National Agency Check (NAC) and a NAC with Written Inquiries (NACI). After the individual applies for a PIV credential, a NAC will be processed. If this does not reveal any unfavorable information, a PIV credential will be issued; this should take about one week. Simultaneously, a NACI will also be initiated, with adjudication taking about six months. If the adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the PIV credentials will be revoked.

Should a contractor's PIV credentials be declined or revoked, the contract administration team must take some action to accommodate this in the contract. For example, the contract may have to be terminated if there is no alternative to on-site performance by the individual in question. On the other hand, it may be possible to arrange off-site performance or some other accommodation. In any case, the contracting officer must work together with the sponsor, security personnel, and the contractor to address this situation promptly.

All PIV credentials will automatically have a five year expiration, except for foreign nationals. Foreign nationals' cards may be issued for five years, unless that date would extend past the

expiration date of their work permit or visa. Governmentwide, the HSPD-12 clearance process for foreign nationals has not been finalized yet. Please be aware that there may be extra delay in obtaining verification for these individuals, especially during the early months of implementation.

If contractor personnel have already been investigated by another agency through OPM, the results of a prior HSPD-12 (or higher) clearance will be accepted by DOI upon receipt of appropriate verification.

Contracting Procedures. Early coordination with requisitioners is recommended in order to avoid delays in contract start-up. Contractors who already have badges may continue to use them until they naturally expire. However, there will be (at least) a week delay for individuals who start unsupervised physical or logical access for the first time on or after October 27.

For now, the background investigations must be paid for by the Government. A source of funding has not been clearly defined, but it appears likely that the sponsoring program will bear the cost. Some program offices may not be aware of this yet. They should be referred to the Bureau's budget office for further guidance. We recommend that solicitations and contracts address limiting the number of contractor employees who will be investigated.

Contracting Officer's Representatives (CORs) will have additional duties, which should be reflected in the COR appointment letter. CORs will act as sponsors for contractor personnel. In this capacity, they will be responsible for ascertaining the risk level for the position, including credentialing requirements in Statements of Work, validating individuals' need for a PIV credential, facilitating the badging process, and ensuring that credentials are renewed and rescinded in a timely manner. It is the COR's responsibility to make sure that contractors' credentials are returned to the Government at the end of the contract or whenever a contractor employee's affiliation with DOI ends.

Model Section C language is attached. The language may be modified to suit circumstances, except that the flow down requirement must be included. It should be used in all contracts where the requisitioner needs contractor personnel to have routine and regular unsupervised access to a Federally controlled facility for more than 180 days or unsupervised access to a Federally controlled Level 3 or 4 information system. It should rarely be applicable to contracts for supplies. When contracting on behalf of other agencies, language from the requisitioning agency that serves the same purpose may be used.

In addition to new contracts, HSPD-12 requirements must be added to some contracts awarded prior to this DIAPR's issuance. Current contracts that require contractor personnel to have physical and/or logical access as described above must be modified to include the PIV requirements when an option is exercised, or before expiration when the contract term (i.e., the need for contractor access) extends past the expiration date of their current credentials. Contracts that do not currently require contractor personnel to have physical and/or logical access as described above must be modified to include the HSPD-12 requirements if circumstances change such that contractor physical or logical access is newly required.

5. **Action Required**:
Distribute this DIAPR as widely as possible, including to requisitioners. Coordinate with program offices and other requisitioners to ensure that the new procedures are followed and that contract work is not delayed. Starting immediately, insert language substantially similar to the attached model language in solicitations that require contractor personnel to have physical or logical access as described above. At the earliest opportunity, but no later than exercise of an option, modify applicable contracts to include language substantially similar the new model language.

6. **Additional Information**: If you have questions about this matter, please contact Dee Emmerich at (202) 208 3348 or delia_emmerich@os.doi.gov.

//s//

Debra E. Sonderman, Director
Office of Acquisition and Property Management

Attachment

Attachment

Model Statement of Work/Performance Work Statement Language

Contractor Personnel Security and Suitability Requirements

Performance of this contract requires contractor personnel to have a Federal government-issued personal identification card before being allowed unsupervised access to a DOI [facility and/or information system]. The Contracting Officer's Representative (COR) will be the sponsoring official, and will make the arrangements for personal identify verification and card issuance.

At least two weeks before start of contract performance, the Contractor will identify all contractor and subcontractor personnel who will require [physical and/or logical] access for performance of work under this contract. The Contractor must make their personnel available at the place and time specified by the COR in order to initiate screening and background investigations. The following forms, or their equivalent, may be used to initiate the credentialing process:

- OPM Standard Form 85 or 85P
- OF 306
- Fingerprint card (local procedures may require the fingerprinting to be done at a police station; in this case, any charges are to be borne by the contractor.)
- Release to Obtain Credit Information
- PIV card application (web-based)

Contractor employees are required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the contractor personnel being screened or investigated in person, by telephone or in writing, and the Contractor agrees to make them available for such contact.

Alternatively, if an individual has already been credentialed by another agency through OPM, and that credential has not yet expired, further investigation may not be necessary. Provide the COR with documentation that supports the individual's status.

During performance of the contract, the Contractor will keep the COR apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the COR and Issuing Office within 24 hours. Replacement will be at the contractor's expense. If reissuance of expired credentials is needed, it will be coordinated through the COR.

At the end of contract performance, or when a contractor employee is no longer working under this contract, the Contractor will ensure that all identification cards are returned to the COR. Before starting work under this contract, a National Agency Check (NAC) will be conducted to

verify the identity of the individual applying for clearance. Upon successful completion of the NAC process, an identification card will be issued and access granted.

Simultaneously, a NAC with Inquiries (NACI) will be initiated to determine the individual's suitability for the position. If the NACI adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the credentials will be revoked. In the event of a disagreement between the Contractor and the Government concerning the suitability of an individual to perform work under this contract, DOI shall have the right of final determination.

This requirement must be incorporated into any subcontracts that require subcontractor personnel to have routine and regular unsupervised access to a Federally controlled facility for more than 180 calendar days or unsupervised access to a Federally controlled Level 3 or 4 information system.

Attachment 4 – Credential Request Form

Instructions for Personal Identity Verification Credential Request form

All information must be legibly printed in blue or black ink.
Forms with strikethroughs or white-out will not be accepted.
All signatures must be original signatures, no copies or stamped signatures.

Sponsors / Registrars / Issuers should maintain a log of all applicant forms they sign (Name, badge type, and date). When the information is entered into the electronic PIV system you maybe asked to digitally sign the forms of applicants that you have processed through the manual (paper-based) process.

Once the Sponsor signs the form, the form should never be given to the applicant except to fill in applicant information in the presence of the Registrar or Issuer.

Sponsor

Complete lines 1 – 10 about the applicant, lines 11 – 13 about yourself, and sign and date line 14. Send the form to your designated Registrar's office.

Line 2 Legal Name of Applicant: - Last, First Middle names – as they appear on official documents (identity proofing source documents)

Line 3 Affiliation:

Employee – Permanent DOI employee
Temporary Employee – Temporary employee/intern paid or obtaining some type of benefit directly from DOI
Contractor – an individual working, under contract, for DOI
Retiree – Retired DOI employee
Volunteer – a non-paid individual working under the supervision of DOI

Line 4 Citizenship: If applicant is not a U.S. citizen please note the country of citizenship and verify that the applicant has been a resident of the United States for at least the last 3 years. If the applicant has not been a resident of the U.S. for at least 3 years, they may not qualify for a PIV card due to restrictions associated with the background investigation. Please contact your Bureau Personnel Security Specialist for further information. Also note, the expiration of their ID cannot extend past the expiration date of their INS documents (i.e., work permit, visa, etc.).

Line 5 Employee Title – Only for permanent employees of DOI

United States Government – used for employees without a specific title listed below and temporary employees, contractors, retirees, and volunteers. This is the default title for the area above the photo on the PIV cards.
LE (Law Enforcement) – DOI employees who are sworn Law Enforcement Officers
Firefighter – Individuals who are employed by DOI in a firefighter capacity.

Security – DOI employee in 080 job series
Investigator – DOI employee in 1801 and 1810 job series

Line 6 Federal Emergency Response Official - Must be approved by Bureau/Office Law Enforcement Director – submit Form XXX

Line 7 Bureau: - bureau name that will appear on the applicant's card

Bureau of Land Management	Bureau of Indian Affairs
Bureau of Reclamation	Minerals Management Service
National Business Center	National Indian Gaming Commission
National Parks Service	U.S. Fish and Wildlife Service
United States Geological Survey	Office of Surface Mining
Office of the Inspector General	Office of the Secretary
Office of the Solicitor	

Lines 8 & 9 – Work address: – Duty station location

Line 10 Contractor Company / Contract Number – for contractors only

Registrar

When applicant arrives in your office, have the applicant complete lines 15 – 19 and sign and date line 20. Verify identity source documents (see attached list of acceptable documents), record the document information, and attach a copy of the documents to the request form. One of the documents must be a State or Federal issued photo ID.

If the applicant is not a U.S. citizen, verify that "No" has been checked on Line 4 and ensure that the applicant has been a resident of the U.S. for at least the past 3 years. If the applicant's INS documentation expires in less than 5 years from the application date, circle the expiration date of the document in red. The PIV card cannot be issued with an expiration date that is later than the date the applicant is legally allowed to reside and work in the U.S.

When the NAC (FBI Fingerprint check) has been completed and successfully adjudicated, the Registrar must fill in lines 36 – 38 and sign and date line 39. Ensure that the applicant's photo has been sent to the designated Issuer.

Line 16 Applicant Physical Characteristics:

Hair color: Auburn, Bald, Black, Blond, Brown, Gray, Red, White,
Eye Color: Black, Blue, Brown, Green, Gray, Hazel
Height – Feet and Inches
Weight - in pounds

Lines 21- 28 Identity Source Documents: - List of acceptable documents is on the last page of these instructions. Copies of both identity source documents must be attached to the PIV request form.

One of the documents must be a State or Federal issued photo ID
Lines 21 & 25 - Name of the applicant as it appears on the document

Lines 23 & 27 – Name of department or agency that issued the document

Line 29 Picture taken: – photo must be sent to Issuer (Polaroid for DI-238A/ DI-238 and digital for others). Registrar must also digitally store picture for later use in smartcard issuance.

Line 30 Fingerprints taken or received: Fingerprints can either be done digitally or on the paper cards. Ensure the correct fingerprint card was used; Employees use SF-87 and Contractors use FD-258.

Line 31 Background Investigation Application Forms Complete: Background Investigation (BI) forms are required for new applicants. If the applicant is a current DOI employee or affiliate, verify that as least a NACI has been completed and is on file. If there is not any record of a NACI for the applicant, they must complete the BI forms. BI forms include SF-85, SF-85P with Credit Report Release, or SF-86 and OF-306. The minimum investigation for the issuance of a PIV credential is a National Agency Check with Inquiries (NACI) and the NAC portion must be completed prior to the issuance of the card. For a NACI an employee needs to complete the SF-85 and a contractor or other affiliate must complete an SF-85P. To receive an advanced NAC (Fingerprint check results) you must make sure that code #3 is placed in block B "Extra Coverage" of the SF-85, SF-85P, or SF-86.

Lines 32 – 35 NAC Adjudication Results: Adjudication of the NAC, which includes the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII) and the FBI National Criminal History Fingerprint Check, must be complete before the PIV card can be issued. If the results are not received within 5 days, the PIV credential may be issued based upon the results of the FBI National Criminal History Fingerprint Check (OMB memo M05-24).

Issuer

The issuer is responsible for issuing the PIV credential, only after Sections A, B, & C are complete and signed. The Issuer must verify the identity of the applicant by comparing the ID to the attached source documents and the source document presented by the applicant at the time of issuance. The Issuer then completes lines 43 – 45 and signs and dates line 46. The Issuer must then have the applicant sign for the receipt of the PIV credential.

Lines 40 – 42 PIV credential information: - Fill in the name on the credential, the credential serial number, and the expiration date printed on the credential. Verify that the expiration date is not greater than 5 years from the issuance date and that the expiration date does not exceed the expiration date of the INS documents for non-U.S. citizens.

LIST OF ACCEPTABLE DOCUMENTS

List A	List B	List C
U. S. Passport (unexpired or expired)	Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
Certificate of U.S. Citizenship (Form N-560 or N-561)	ID card issued by Federal, State or local government agencies of entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	Certification of Birth abroad issued by the Department of State (form FS-545 or Form DS-1350)
Certificate of Naturalization (Form N-550 or N-570)	School ID card with a photograph	Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal.
Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	Voter's registration card	Native American tribal document
Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-551)	U.S. Military card or draft record	U.S. Citizen ID Card (Form I-197)
Unexpired Temporary Resident Card (Form I-688)	Military dependent's ID card	ID Card for use of Resident Citizen in the United States (Form I-179)
Unexpired Employment Authorization Card (Form I-688A)	U.S. Coast Guard Merchant Mariner Card	Unexpired employment authorization document issued by DHS (other than those listed under List A)
Unexpired Reentry Permit (Form I-327)	Driver's license issued by a Canadian government authority	
Unexpired Refugee Travel Document (form I-571)	**For persons under age 18 who are unable to present a document listed above**:	
	School record or report card	
	Clinic, doctor or hospital record	
	Day-care or nursery school record	

Attachment 2 – Financial Assistance

October 24, 2005

Financial Assistance Communication Liaison Policy Release: 2006 - 1

To: Bureau/Office Financial Assistance Communication Liaisons

Subject: Implementation of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Financial Assistance Awardees

1. **Purpose**: This policy release establishes procedures for standard implementation of HSPD-12 in Department of the Interior financial assistance (i.e., grants and cooperative agreements).

2. **Effective Date**: Upon signature.

3. **Expiration Date**: Upon issuance of applicable Office of Management and Budget policy coverage.

4. **Background and Explanation**:
HSPD-12, issued on August 27, 2004, directs the creation of a new Federal standard for secure and reliable identification issued by Federal agencies to their employees and contractors, including all tiers of subcontractors, and financial assistance recipients. Implementation will be in several stages, with the initial phase being put in place on October 27, 2005. This first phase consists of implementation of procedures under which Personal Identity Verification (PIV) credentials such as security badges, building passes, and so forth, will only be issued after an individual's identity has been independently verified. Later phases will expand coverage to personnel who have already been issued credentials as of October 27, and use of Smart Cards.

Not every financial assistance recipient and subrecipient (hereafter, "recipient") employee will need PIV credentials. There are two categories of recipient personnel who will be subject to the background investigations:

- Those who need routine and regular unsupervised access to a Federally controlled facility for more than 180 days;
- Those who need unsupervised access to a Federally controlled Level 3 or 4 information system.

Physical Access. A "Federally controlled facility" is federally owned or leased space, whether for single or multi-tenant occupancy, all or any portion of which is under the jurisdiction, custody or control of DOI. If a building is shared with non-government tenants, only access to the Federal area is controlled. The requirements for recipient credentialing apply even if there is no guard, card reader, or other physical control at the entrance to the office. The 180 calendar day period begins on the first day of the individual's affiliation with DOI (in this case, the date that grant or cooperative agreement performance actually begins rather than the grant or cooperative agreement award date) and ends exactly 180 days later, regardless of the number of times the recipient actually accessed a building or IT system.

Logical Access. An "information technology system" is defined in the Federal Information Security Management Act of 2002 (44 U.S.C. §3503(8)). Use of an information system by a recipient or contractor on behalf of an agency is defined in 44 U.S.C. §3544(a)(1)(A). If a recipient needs *any* amount of unsupervised access to a DOI IT system, HSPD-12 compliant credentials must be issued regardless of the duration of access. The credentialing requirement applies whether the recipient accesses the IT system from the premises of a DOI facility, from their own facility, through the Internet, or by any other means.

Uncredentialed Recipients. Recipients who do not fit into one of the above two categories will be treated as visitors. These persons must access the facility via a screening system, display a temporary/visitor badge at all times, and be escorted at all times. Normally, persons working exclusively outside on the grounds of federally controlled facilities need not receive background investigations.

Special Cases. The preceding paragraphs describe the minimum requirements. Depending on risk, increased application of HSPD-12 will be appropriate in some cases, depending on the nature of the grant/cooperative agreement. If higher level security, such as Secret or Top Secret, is needed, other clearances can be added to the HSPD-12 requirements.

Verification Process. To the extent possible, HSPD-12 clearance of recipient personnel will be handled through the same clearance procedures as for Department of the Interior employees. The process has two steps: a National Agency Check (NAC) and a NAC with Written Inquiries (NACI). After the individual applies for a PIV credential, a NAC will be processed. If this does not reveal any unfavorable information, a PIV credential will be issued; this should take about one week. Simultaneously, a NACI will also be initiated, with adjudication taking about six months. If the adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the PIV credentials will be revoked.

Should a recipient's PIV credentials be declined or revoked, the grant/cooperative agreement administration team must take some action to accommodate this in the grant/cooperative agreement. For example, it may be possible to arrange off-site performance or some other accommodation. In any case, the administering office must

work together with the sponsor, i.e., program office, security personnel, and the recipient to address this situation promptly.

All PIV credentials will automatically have a five year expiration, except for foreign nationals. Foreign nationals' cards may be issued for five years, unless that date would extend past the expiration date of their work permit or visa. Governmentwide, the HSPD-12 clearance process for foreign nationals has not been finalized yet. Please be aware that there may be extra delay in obtaining verification for these individuals, especially during the early months of implementation.

If recipient personnel have already been investigated by another agency through OPM, the results of a prior HSPD-12 (or higher) clearance will be accepted by DOI upon receipt of appropriate verification.

Procedures. Early coordination with program officials is recommended in order to avoid delays in grant/cooperative agreement start-up. Recipients who already have badges may continue to use them until they expire. However, there will be (at least) a week delay for individuals who start unsupervised physical or logical access for the first time on or after October 27.

For now, the background investigations must be paid for by the Government. A source of funding has not been clearly defined, but it appears likely that the sponsoring program will bear the cost. Some program offices may not be aware of this yet. They should be referred to the Bureau's budget office for further guidance. We recommend that grant/cooperative agreement applications address limiting the number of recipient employees who will be investigated.

DOI grant/cooperative agreement office personnel will have additional duties, which should be reflected in the application process. DOI personnel will act as sponsors for recipient personnel. In this capacity, they will be responsible for ascertaining the risk level for the position, including credentialing requirements in the grant/cooperative agreement descriptions, validating individuals' need for a PIV credential, facilitating the badging process, and ensuring that credentials are renewed and rescinded in a timely manner. It is the DOI grant/cooperative agreement office's responsibility to make sure that recipients' credentials are returned to the Government at the end of the grant/cooperative agreement or whenever a recipient employee's affiliation with DOI ends.

Model Special Terms and Conditions language is attached. The language may be modified to suit circumstances, except that the flow down requirement must be included. It should be used in all grants and cooperative agreements where the terms require subrecipient personnel to have unsupervised access to a Federally controlled facility for more than 180 days or unsupervised access to a Federally controlled Level 3 or 4 information system.

In addition to new grants and cooperative agreements, HSPD-12 requirements must be added to some grants and cooperative agreements awarded prior to this policy release's issuance. Current grants or cooperative agreements that require recipient personnel to have physical and/or logical access as described above must be amended to include the PIV requirements before expiration when the grant/cooperative agreement extends past the expiration date of their current credentials. Grants or cooperative agreements that do not currently require recipient personnel to have physical and/or logical access as described above must be modified to include the HSPD-12 requirements if circumstances change such that recipient physical or logical access is newly required.

5. **Action Required**:
Coordinate with DOI grant\cooperative agreement offices to ensure that the new procedures are followed and that grant or cooperative agreement work is not delayed. Starting immediately, insert language substantially similar to the attached model language in applications that require recipient personnel to have physical or logical access as described above. At the earliest opportunity, but no later than exercise of an amendment, amend applicable grants and cooperative agreements to include the new model language. Distribute this policy release as widely as possible within your bureau/office grants and cooperative agreements community.

6. **Additional Information**: If you have questions about this matter, please contact Kate Oliver at (202) 208-3345 or kate_oliver@ios.doi.gov.

//s//

Debra E. Sonderman, Director
Office of Acquisition and Property Management

Attachment

Attachment

Model HSPD-12 Grant/Cooperative Agreement Language

Recipient/Subrecipient Personnel Security and Suitability Requirements

Performance of this grant/cooperative agreement requires recipient/subrecipient personnel to have a Federal government-issued personal identification card before being allowed unsupervised access to a DOI [facility and/or information system]. _____ [to be completed by bureau/office, e.g., designated grants/cooperative agreement administrator] will be the sponsoring official, and will make the arrangements for personal identify verification and card issuance.

At least two weeks before start of grant/cooperative agreement performance, the recipient will identify all recipient and subrecipient personnel who will require [physical and/or logical] access for performance of work under this grant/cooperative agreement. The recipient and subrecipient must make their personnel available at the place and time specified by the _____[title to be completed by the bureau/office] in order to initiate screening and background investigations. The following forms, or their equivalent, may be used to initiate the credentialing process:

- OPM Standard Form 85 or 85P
- OF 306
- Fingerprint card (local procedures may require the fingerprinting to be done at a police station; in this case, any charges are to be borne by the recipient or subrecipient, as applicable)
- Release to Obtain Credit Information
- PIV card application (web-based)

Recipient and subrecipient employees are required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the recipient or subrecipient personnel being screened or investigated in person, by telephone or in writing, and the recipient agrees to make them available for such contact.

Alternatively, if an individual has already been credentialed by another agency through OPM, and that credential has not yet expired, further clearance may not be necessary. Provide the sponsoring office with documentation that supports the individual's status.

During performance of the grant/cooperative agreement, the recipient will keep the _____[title to be completed by the bureau/office] apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the _____[title to be completed by the bureau/office] and Issuing Office within 24 hours. Replacement will be at the recipient's

expense. If reissuance of expired credentials is needed, it will be coordinated through the _____[title to be completed by the bureau/office].

At the end of grant/cooperative agreement's performance, or when a recipient/subrecipient employee is no longer working under this grant/cooperative agreement, the recipient will ensure that all identification cards are returned to the _____ [title to be completed by the bureau/office].
Before starting work under this agreement, a National Agency Check (NAC) will be conducted to verify the identity of the individual applying for clearance. Upon successful completion of the NAC process, an identification card will be issued and access granted.

Simultaneously, a NAC with Inquiries (NACI) will be initiated to determine the individual's suitability for the position. If the NACI adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the credentials will be revoked. In the event of a disagreement between the recipient and the Government concerning the suitability of an individual to perform work under this grant/cooperative agreement, DOI shall have the right of final determination.

This requirement must be incorporated into any sub-grants/cooperative agreements that require subrecipient personnel to have unsupervised access to a Federally controlled facility for more than 180 calendar days or unsupervised access to a Federally controlled Level 3 or 4 information system.

D R A F T

Attachment 3 – Flow Chart

New Contractor/Other Affiliate PIV Flow Chart
Paper Process October 2005

COR/Sponsor

1. Complete on line training. Retain certificate verifying completion of the training.

2. Completes and sends to Registrar:

   a. PIV Request Form, Section A
   b. 9-3056 (Personnel Security Request Form)
   c. Copy of certificate verifying completed PIV-1 Training.

3. Gives Applicant the following forms to complete. When forms are completed, applicant personally provides forms to Registrar.

   a. SF-85 or SF-85P (along with Credit Report Release)
   b. OF-306
   c. Fingerprint Chart, FD-258
   d. List of Forms on I-9

Registrar

1. Receives the following forms from the COR and applicant:

   a. PIV Request Form
   b. 9-3056 (Personnel Security Request Form)
   c. SF-85 or SF-85P (along with Credit Report Release)
   d. OF-306
   e. Fingerprint Chart, FD-258

2. Conducts identity proofing, verifying two documents from the I-9 (copies must be made of the two identifying documents).

3. Takes applicant's photo and sends to the Issuer with name of applicant.

4. Takes fingerprints of applicant or receives previously completed fingerprint chart.

5. Completes Section B of the PIV Request Form.

6. Sends forms mentioned in Registrar #1, above, along with copies of the two identity proofing documents to the RSOs.

D R A F T

Regional Security Officers

1. Receives the following forms from the Registrar:

    a. PIV Request Form
    b. 9-3056 (Personnel Security Request Form)
    c. SF-85 or SF-85P (along with Credit Report Release)
    d. OF-306
    e. Fingerprint Chart, FD-258
    f. Copies of the two identity proofing documents

2. Ensures that 9-3056 is complete. Signs 9-3056.

3. Reviews SF-85 or SF-85P for accuracy and completeness. Completes top portion of SF-85 or SF-85P for signature by Security Management Office.

4. Completes Section C of the PIV Request Form.

5. Sends forms mentioned in Regional Security Officer #1, above, to the Security Management Office.

Security Management Office

1. Receives the following forms from the Regional Security Officers:

    a. PIV Request Form
    b. 9-3056 (Personnel Security Request Form)
    c. SF-85 or SF-85P (along with Credit Report Release)
    d. OF-306
    e. Fingerprint Chart, FD-258
    f. Copies of the two identity proofing documents

2. Requests background investigation from OPM, creates file, and enters into PSCS database.

3. Adjudicates the Advanced NAC.

4. Processes PIV based on NAC results:
    a. If NAC is negative, returns information to COR/Sponsor.
    b. If NAC is positive, completes Section D of the PIV Request Form and sends PIV form to the Issuer (keep copy of PIV form).

Issuer

1. Receives PIV Request Form from the Security Management Office.

2. Obtains Badge Form from Authorized Designated Issuing Officers for Identification Cards.

3. Places applicant photo, which was previously sent by the Registrar, on the Badge Form.

4. Contacts COR Sponsor that the card is ready. COR/Sponsor notifies contractor/ applicant that badge is ready for pickup and specifies Issuer location.

5. Contractor/Applicant appears to Issue, who verifies identity using identity source document presented by the applicant.

5. Completes Section E of the PIV Request Form.

6. Obtains a signature from the applicant on the PIV Request Form, Section F.

7. Gives completed Badge Form to applicant.

8. Sends completed PIV form to the Security Management Office for record retention.

L:\ofms\so\share\PIV Contractor Flow Chart

Attachment 5 – Request for PIV Credential

Request for DOI Personal Identity Verification (PIV) Credential

Pursuant to Section 3(e)(3) of the Privacy Act of 1974 (Public law 93-573), the individual furnishing information on this form is hereby advised as follows: 1. The authority for solicitation of the information is 5 U.S.C. 301, Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995, and Homeland Security Presidential Directive – 12, August 27, 2004. 2. The principle purposes for which the information is intended to be used are: (a) To ensure the safety and security of DOI facilities and their occupants in which the system is installed; (b) To verify that all persons entering DOI facilities or other Government facilities with smart card systems are authorized to enter them; and (c) To track and control ID security cards issued to persons entering and exiting the facilities. 3. The routine uses of the information are: (a) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs, on DOI's behalf, services requiring access to these records; (b) To the Federal Protective Service and appropriate Federal, State, local or foreign agencies responsible for investigating emergency response situations or investigating or prosecuting the violation of or for enforcing or implementing a statute, rule, regulation, order or license, when DOI becomes aware of a violation or potential violation of a statute, rule, regulation, order or license; (c) To another agency with a similar smart card system when a person with a smart card desires access to that agency's facilities; and (d) To those identified in the Department of the Interior system of records notice: Interior, Computerized ID Security System, OS-1. A copy is available on the Department of the Interior Privacy Program website at www.doi.gov/ocio/privacy. 4. The effect on the individual of not providing all or any part of the requested information may result in disapproval of the issuance of the PIV ID credential.

A. Sponsor/COR - PIV Request

1. Replacement Card? ☐ No ☐ Yes: 1a. Reason for Replacement_____
2. Legal Name (L,FM): _____ Phone Number _____
3. Affiliation: ☐ Employee ☐ Temporary Employee ☐ Contractor ☐ Retiree ☐ Volunteer
4. U.S. Citizen? ☐ Yes ☐ No: 3a. Country of Citizenship _____
5. Employee Title: ☐ U.S. Government ☐ LE ☐ Firefighter ☐ Security ☐ Investigator
6. Federal Emergency Response Official? ☐ (Must be approved by Bureau/Office Law Enforcement Director)
7. Bureau: _____ Office: _____
8. Work Address: _____
9. City: _____ State: _____ Zip: _____
10. Contractor Company: _____ Contract Number: _____

Sponsor Information

11. Name: _____ Phone Number: _____
12. Organization: _____ Title: _____
13. Email: _____

I agree to sponsor the above application for a PIV credential and certify that the information is accurate to the best of my knowledge.

14. Sponsor/COR Signature: _____ Date (mm/dd/yyyy): _____/___/_____

B. Registrar - Source Document Confirmation, Applicant's Picture, and Fingerprints (Only for New Cards after Section A is completed)

Applicant Information

15. Birth date (mm/dd/yyyy): _____/____/_____
16. Hair Color _____ Eye Color _____ Height _____ Weight _____ Gender_____
17. Home Address: _____
18. City: _____ State: _____ Zip: _____
19. Email: _____

I certify that the information is accurate to the best of my knowledge.

20. Applicant Signature: _____ Date (mm/dd/yyyy): _____/____/_____

Identity Source Document 1 (Attach copy)

21. Name: _____
22. Document #: _____Document Title: _____
23. Issuer: _____

24. Document Expiration Date (mm/dd/yyyy): _____/____/_____

Identity Source Document 2 (Attach copy)

25. Name: _____

26. Document #: _____ Document Title: _____

27. Issuer: _____

28. Document Expiration Date (mm/dd/yyyy): _____/____/_____

Applicant's Picture

29. Picture taken? ☐ Yes

30. Fingerprints taken or received? ☐ Yes (Employees – SF-87) (Contractors – FD-258)

31. Background Investigation Application Forms Complete? ☐ Yes (required for new cards only)

C. Human Resources /Security Management Office

NAC Adjudication Results

32. Date Completed (mm/dd/yyyy): _____/____/_____

33. Successful? ☐ Yes ☐ No

34. Comments: _____

_____

I certify that the information regarding the above applicant is accurate to the best of my knowledge and approve this applicant for credential issuance.

35. Human Resources/Security Management Office Signature: _____

Date (mm/dd/yyyy): _____/____/_____

Registrar Information

36. Name: _____Phone Number: _____

37. Organization: _____ Title: _____

38. Email: _____

I hereby confirm that the information contained in the above documents were checked and verified and the FBI fingerprint results have been successfully adjudicated.

39. Registrar Signature: _____ Date (mm/dd/yyyy): _____/____/_____

D. Issuer (To be completed by Issuer, after Sections A, B, and C are completed))

40. Name on Credential: _____

41. Credential Identifier: _____

42. Credential Expiration Date (mm/dd/yyyy): _____/____/_____

Issuer Information

43. Name: _____ Phone Number: _____

44. Organization: _____ Title: _____

45. Email: _____

I hereby acknowledge issuance of a credential to the applicant identified above based on verification of the applicant's identity and verification of the above Registrar's issuance approval.

46. Issuer Signature: _____ Date (mm/dd/yyyy): _____/____/_____

E. Applicant Acknowledgement (To be completed by Applicant, after Section D is completed)

I, the Applicant, confirm receipt of the PIV credential identified above and that the information is accurate to the best of my knowledge, and agree to abide by all rules and responsibilities associated with this credential.

47. Applicant Signature: _____ Date (mm/dd/yyyy): _____/____/_____